Dealing with blockchain technology for Incident Response

By Sam Perl

CMU Heinz College, Dietrich College, SEI CERT, FIT

Speaker Introduction: Sam Perl

Carnegie Mellon University
HeinzCollege
INFORMATION SYSTEMS • PUBLIC POLICY • MANAGEMENT

Dietrich College of
Humanities and
Social Sciences

Carnegie
Mellon
University
Software
Engineering
Institute

FLORIDA
TECH

- Heinz College, Instructor
  - 95-810 Blockchain Fundamentals
- Dietrich College Instructor
  - 67-309 Special Topics Information Assurance
- SEI CMU CERT Senior Member of the Technical Staff
  - Security Operations
  - CSIRT Development and Training Team
- Florida Institute of Technology, Graduate Advisor
  - Thesis Projects

Agenda

1. **Review fundamentals** of Blockchain technology for Incident Responders
2. **Show examples** of blockchain based technology projects such as Smart Contracts.
3. **Discuss impacts** a few blockchain examples has on incident management.
4. **Speculate** how the technology may affect the future workload of Incident Responders and Coordination Centers.

Key Blockchain Technology Terms

Blockchain Networks – Public (Decentralized) and Private Ledger Systems

Cryptocurrencies – Bitcoin, Ethereum, Solana, Algorand

Wallets – Solutions to manage various Public Key, Private Key pairs, identity addresses, and user interactions

Layer 2 – Networks on top of blockchain that enable ‘Payment’ (and other) services. Example: Lightning

Smart Contracts – Executable code running on Blockchains

Web3 - Decentralized Applications (dAPPs) running on Smart Contracts and other technology

‘Smart Contract’ Definition

- Terms of agreement in Code
- The code can be automatically triggered by signed blockchain transactions
- **Used to govern transfer of digital currency, tokens, assets, control access to data (such as music) or other information.**
- Smart contracts are computer programs. (They are more like legal ‘agreements’ until their enforcement is litigated/clarified…)

Sources:
- De Filippi, Primavera De Filippi. "Blockchain and the Law." *Blockchain and the Law*. Harvard University Press, 2018.. Chapter 4 Smart Contracts as Legal Contracts
- Antonopoulos, Andreas M., and Gavin Wood. Mastering ethereum: building smart contracts and dapps. O'reilly Media, 2018.

Approaching Incident Response for Blockchain related Activity

- **Primary Focus: How might traditional Incident Response teams deal with Blockchain related issues?**

- Second but related: How do teams respond to Attacks on blockchain networks, software, users, applications, etc. ?

What happens when an IR team runs into a Blockchain?

The next few slide show some examples of incidents involving blockchains.

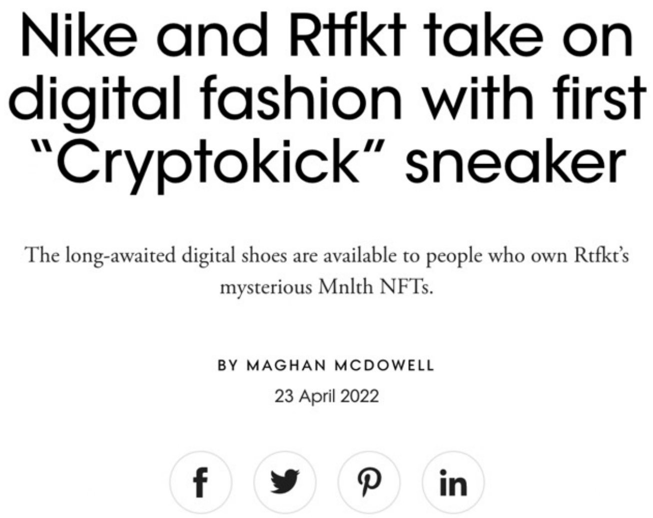
For each example, please ask yourself:

- How might your team respond?
- What skills would your team need to have to do so?
- What contacts or relationships would you want & with who(m)?
- If you need specialized help or support, would you know who to call?
- Could you collect the right data?
- Would you be able to analyze the data you collect?
- Would your stakeholders be able to understand what you are doing and why ?

Your organization decides to experiment with an NFT project to attract and retain customers.

ENHANCED BY
RTFKT

Photo: Rtfkt x Nike



Nike and Rtfkt take on digital fashion with first "Cryptokick" sneaker

The long-awaited digital shoes are available to people who own Rtfkt's mysterious Mnlth NFTs.

BY MAGHAN MCDOWELL

23 April 2022

Source: McDowell, Maghan, Nike 'Nike and Rtfkt take on digital fashion with first "Cryptokick" sneaker', Vogue Business, April 23, 2022

Quick Technical Primer for an NFT System

Note: your organization is the NFT Owner/Creator in this example. (User-Side)

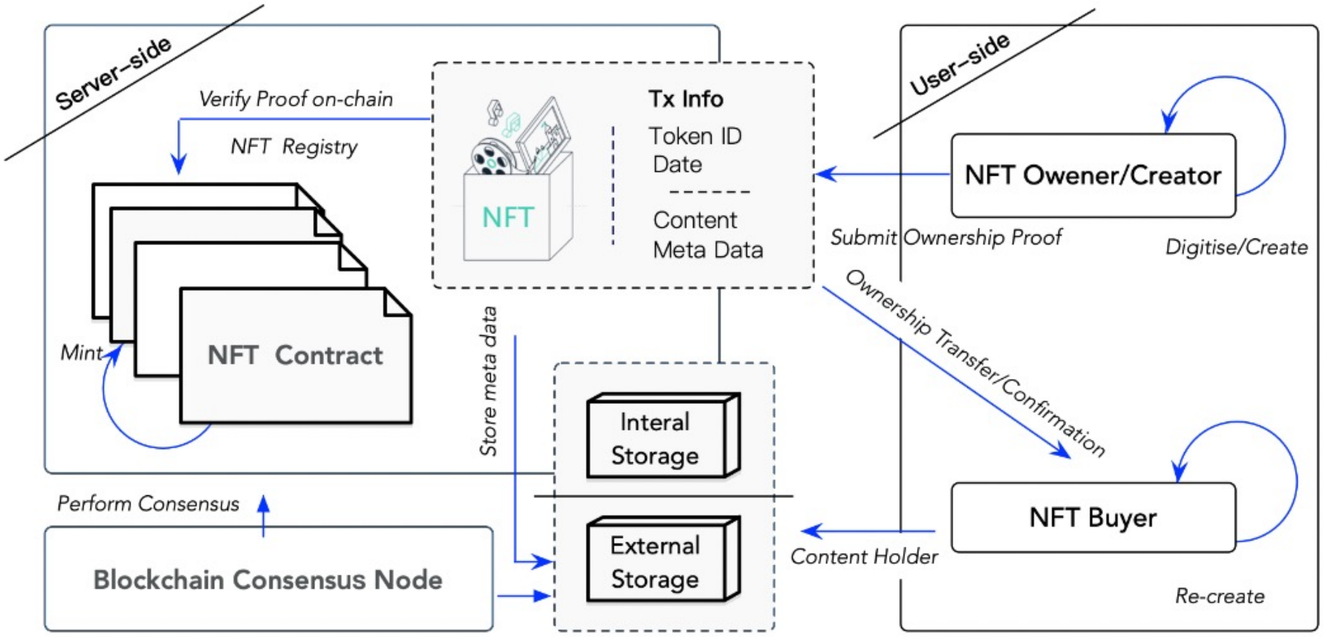


Fig. 1: Workflow of NFT Systems

Source: Wang, Qin, et al. "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges." arXiv preprint arXiv:2105.07447 (2021).

Steps

1. Create, Test

2. Launch, Deploy

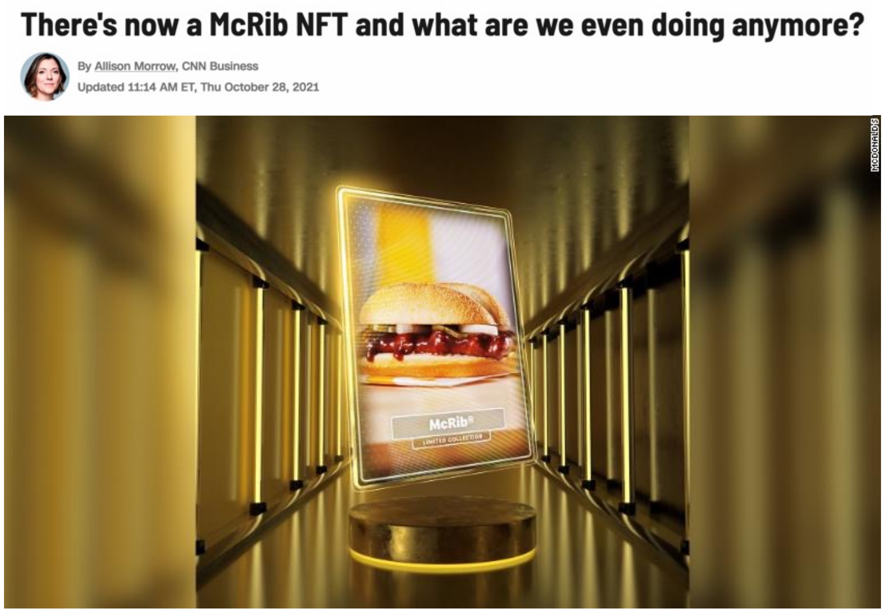
(compile & publish your contract)

3. Mint tokens and distribute them

4. Operate
(Users Buy and Sell your tokens)

The org. puts the NFT on the Ethereum Blockchain

Organizations are using Digital Assets as advertising to attract & retain customers



There's now a McRib NFT and what are we even doing anymore?

By Allison Morrow, CNN Business
Updated 11:14 AM ET, Thu October 28, 2021

Sources:

- Image: https://cdn.cnn.com/cnnnext/dam/assets/211028094602-mcdonalds-mcrib-nft-exlarge-169.jpg
- Morrow, Allison, ”There's now a McRib NFT and what are we even doing anymore?”, CNN Business, October 28, 2021
- McCoy, Elin, “Winemakers are dropping wine NFTs to attract new consumers”, Bloomberg, April 25, 2022
- Strickland, Derek, “Adidas makes $23 million on first NFTs: 'This is just the beginning’”, Tweaktown, December 19, 2021
- Bowler, Hannah, “Pepsi marketing boss ‘bullish’ on the future of NFTs”, The Drum News, March 31, 2022

LIFESTYLE • NFTS

Winemakers are dropping wine NFTs to attract new consumers

(Fortune Magazine)

BY ELIN MCCOY AND BLOOMBERG
April 25, 2022 12:22 PM EDT

Business, Financial & Legal

Adidas makes $23 million on first NFTs: 'This is just the beginning'

Adidas' first Originals NFT line sells out extremely quickly, company has made over 5,900 ETH *($23 million) from the NFT drop.

Derek Strickland
@DeekeTweak

PUBLISHED SUN, DEC 19 2021 2:02 PM CST | UPDATED THU, JAN 13 2022 3:00 AM CST

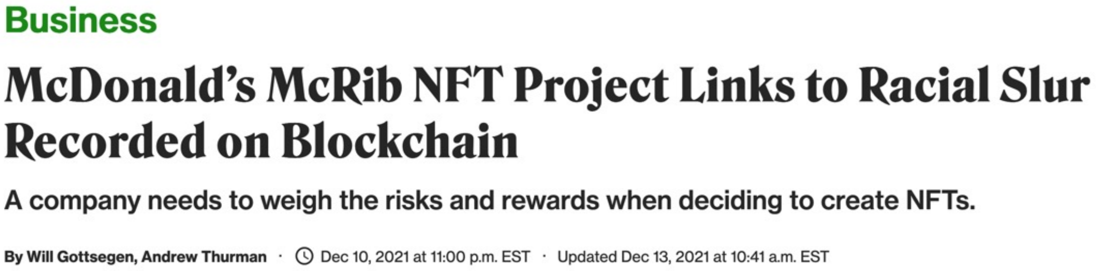
NEWS

Pepsi marketing boss ‘bullish’ on the future of NFTs

By Hannah Bowler - March 31, 2022

The Launch - Example Incident #1

- A user sends the Smart Contract for the NFT a deposit of 0.000069 ETH ($0.20 USD)
- The user includes *additional data* with their transaction (allowed by the protocol)
- Result “[The NFT Smart Contract] allowed someone completely unaffiliated with the project to send [it] offensive language, which is stored on the blockchain publicly.”



Business

McDonald’s McRib NFT Project Links to Racial Slur Recorded on Blockchain

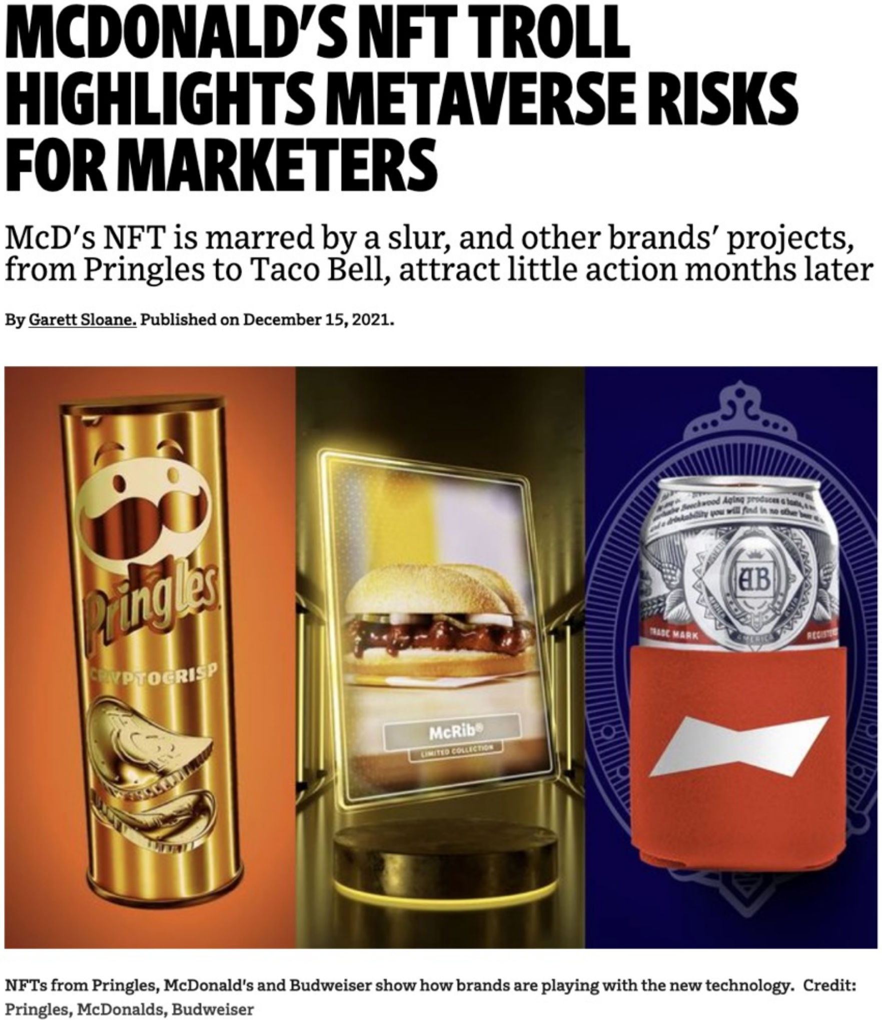
A company needs to weigh the risks and rewards when deciding to create NFTs.

By Will Gottsegen, Andrew Thurman · Dec 10, 2021 at 11:00 p.m. EST · Updated Dec 13, 2021 at 10:41 a.m. EST

Sources:

- Gottsegen, Will and Thurman, Andrew, , “McDonald’s McRib NFT Project Links to Racial Slur Recorded on Blockchain”, December 10, 2021

Could you respond?



MCDONALD'S NFT TROLL HIGHLIGHTS METAVERSE RISKS FOR MARKETERS

McD's NFT is marred by a slur, and other brands' projects, from Pringles to Taco Bell, attract little action months later

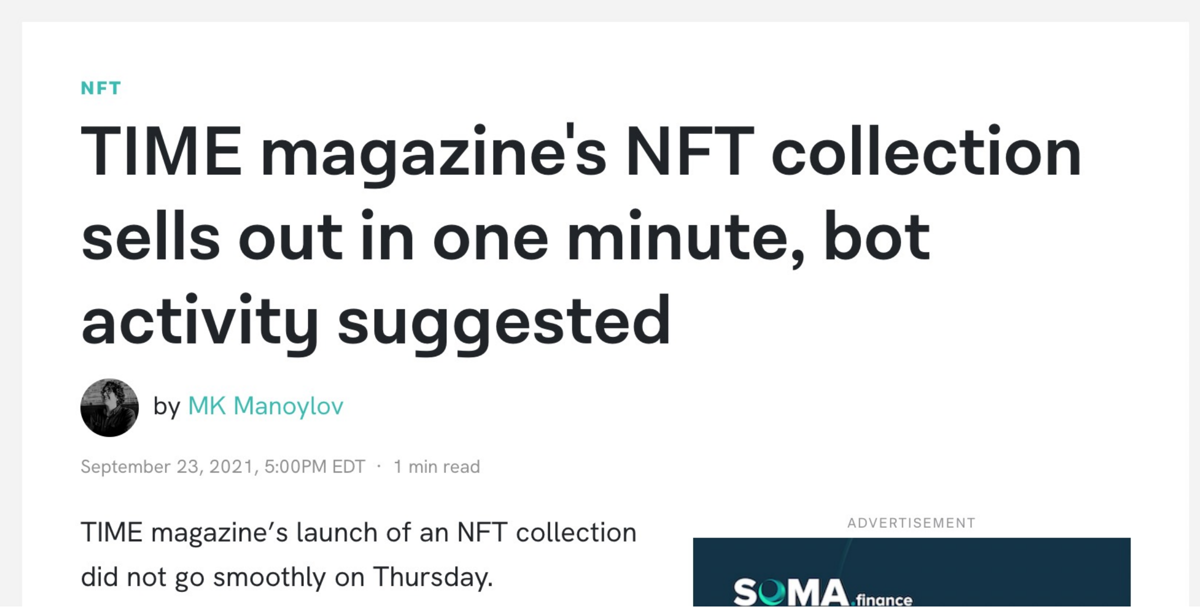
By Garett Sloane. Published on December 15, 2021.

NFTs from Pringles, McDonald's and Budweiser show how brands are playing with the new technology. Credit: Pringles, McDonalds, Budweiser

Source: Sloane, Garret, "McDonald's NFT troll highlights metaverse risks for marketers", AdAge, December 15, 2021

- Technical Response – can you diagnose the problem?
- Understand the Decision Choices?
  - Unable to remove the comments as you can with a company run website
  - Even if you could, Decentralized clients means thousands of copies
  - Users can choose not to update their chains
- What would your procedures be?
- Social Responses?
  - to customers
  - Updates to Stakeholders?
- Smart Contract Analysis?
- Implications of Replacing the Smart Contract?

Here are Launches with “different complications”



NFT

TIME magazine's NFT collection sells out in one minute, bot activity suggested

by MK Manoylov

September 23, 2021, 5:00PM EDT · 1 min read

TIME magazine’s launch of an NFT collection did not go smoothly on Thursday.

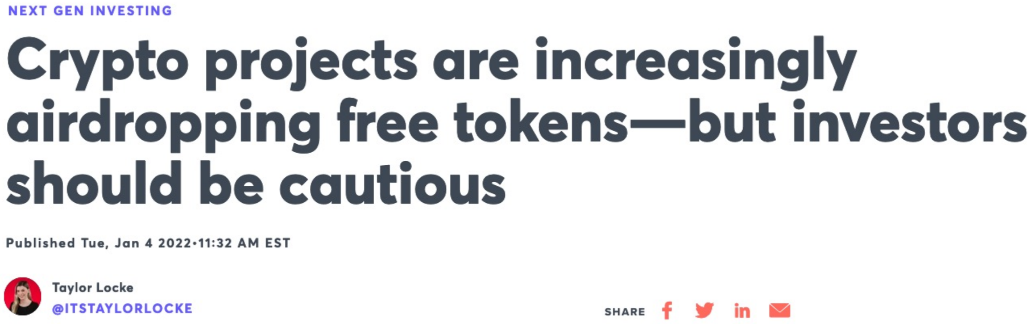
Source: Manoylov, MK, “TIME magazine's NFT collection sells out in one minute, bot activity suggested”, The Block Crypto September 23, 2021

- Target users unable to claim any items
- What protections could have been put in place to prevent the automated claims?
- How to respond now?
  - Manually review all logs, make determinations/guesses as to who is a bot and who is not?
  - New skills needed?

Post Launch Challenges – Incident #2

You make it through the launch but new complications emerge

- After 2 months, a new *DAO* project decides to *Airdrop* new coins to all of the *Wallets* that hold one of your NFTs.
    - DAOs are Decentralized Autonomous Organizations; groups of affiliated users and developers without a required central authority (in theory)
    - Airdrops distribute new ‘free’ tokens of their own project to your token holders
- Your Users/Fans connect their wallets to a Smart Contract to ‘claim’ the drop
- Reasons why people giveaway some NFTs for free: Marketing, Engage with ’power users’, or Signaling/Influence, increase attention for their project



NEXT GEN INVESTING

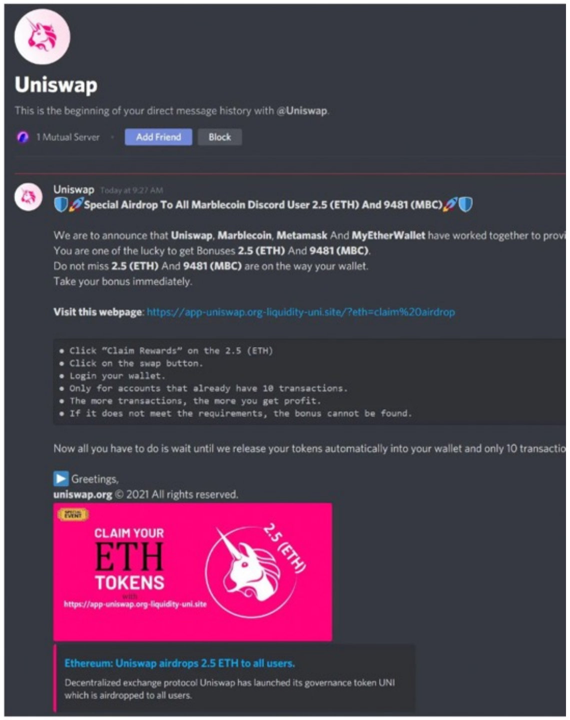
Crypto projects are increasingly airdropping free tokens—but investors should be cautious

Published Tue, Jan 4 2022•11:32 AM EST

Taylor Locke
@ITSTAYLORLOCKE

Source: Locke, Taylor, “Crypto projects are increasingly airdropping free tokens—but investors should be cautious”, CNBC, January 4, 2022

Variations on Phishing / Social Engineering



This is the beginning of your direct message history with **@Uniswap**.

Uniswap Today at 9:27 AM

🛡🚀**Special Airdrop To All Marblecoin Discord User 2.5 (ETH) And 9481 (MBC)**🚀🛡

We are to announce that **Uniswap**, **Marblecoin**, **Metamask** And **MyEtherWallet** have worked together to provi
You are one of the lucky to get Bonuses **2.5 (ETH)** And **9481 (MBC)**.
Do not miss **2.5 (ETH)** And **9481 (MBC)** are on the way your wallet.
Take your bonus immediately.

Visit this webpage: https://app-uniswap.org-liquidity-uni.site/?eth=claim%20airdrop

```
• Click "Claim Rewards" on the 2.5 (ETH)
• Click on the swap button.
• Login your wallet.
• Only for accounts that already have 10 transactions.
• The more transactions, the more you get profit.
• If it does not meet the requirements, the bonus cannot be found.
```

Now all you have to do is wait until we release your tokens automatically into your wallet and only 10 transactio

▶ Greetings,
uniswap.org © 2021 All rights reserved.

Ethereum: Uniswap airdrops 2.5 ETH to all users.

Decentralized exchange protocol Uniswap has launched its governance token UNI which is airdropped to all users.

An excerpt from an airdrop scam post on a discord server.

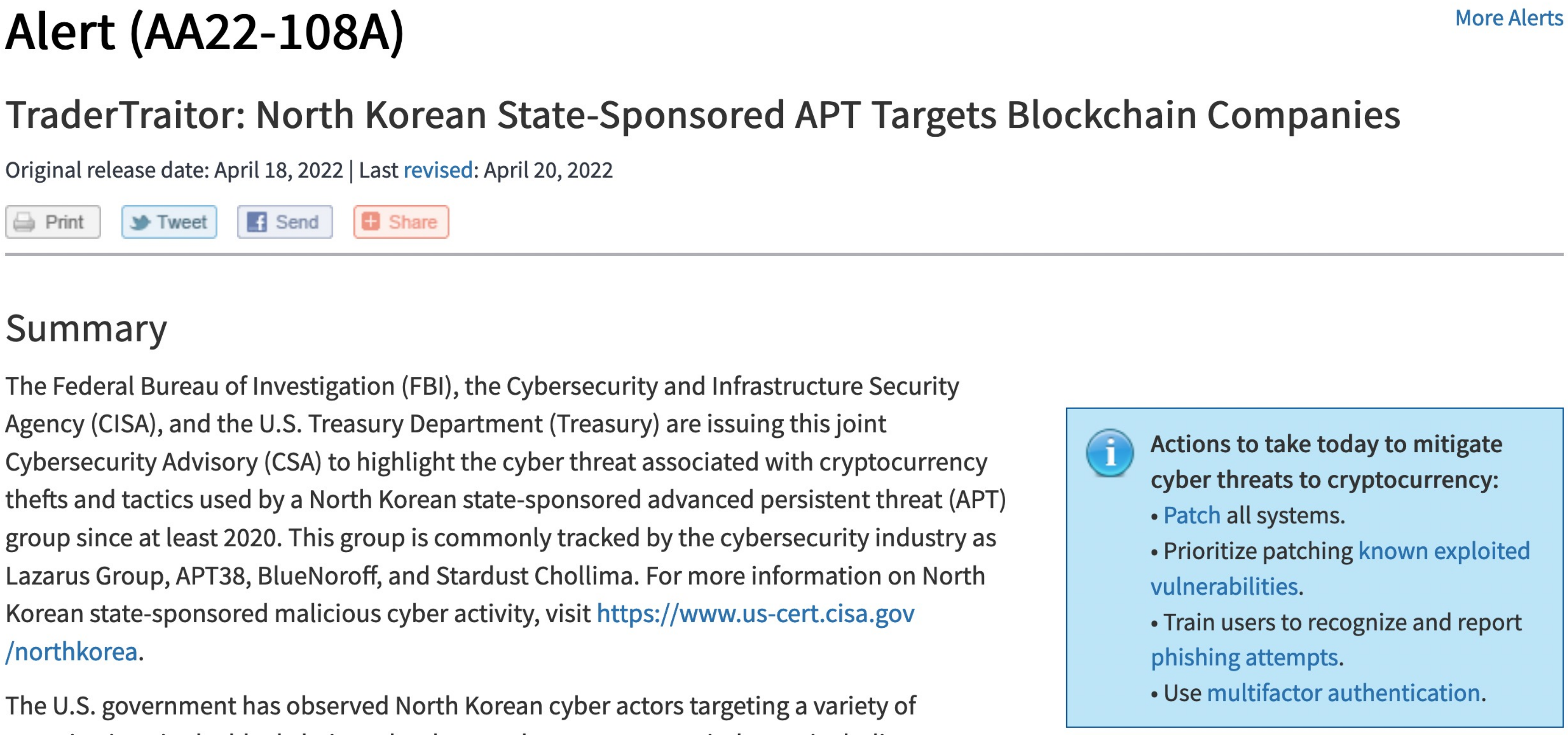
Source: de Candia, Alfredo, "Identifying Uniswap Impersonating Scams on Discord: A Checklist", Hackernoon, March 25, 2021

- Attackers impersonated developers for the Airdrop on the team's Discord
- The attackers sent a fake 'claim' link which turned out to compromise wallets that connected to it.
- Some of your NFT customers fell victim to the Airdrop scam.
- Attackers transferred the NFTs out of your customers' wallets.

Are you able to respond?

- What are your Policies for such situations?
- Communications, Contact Lists?
- Digital Forensics, Blockchain Analysis, Funds Tracking?
- Customer Relations?
- Who is the adversary, what intelligence do you have on them?
- What data sources are you using?
- Can you access the blockchain data? - Do you have the infrastructure & tools & skills to perform the analysis?
- How long will it take to get spun up?

Threat Actors are motivated and active



Alert (AA22-108A)

TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies

Original release date: April 18, 2022 | Last revised: April 20, 2022

Summary

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the U.S. Treasury Department (Treasury) are issuing this joint Cybersecurity Advisory (CSA) to highlight the cyber threat associated with cryptocurrency thefts and tactics used by a North Korean state-sponsored advanced persistent threat (APT) group since at least 2020. This group is commonly tracked by the cybersecurity industry as Lazarus Group, APT38, BlueNoroff, and Stardust Chollima. For more information on North Korean state-sponsored malicious cyber activity, visit https://www.us-cert.cisa.gov/northkorea.

The U.S. government has observed North Korean cyber actors targeting a variety of

Actions to take today to mitigate cyber threats to cryptocurrency:

- Patch all systems.
- Prioritize patching known exploited vulnerabilities.
- Train users to recognize and report phishing attempts.
- Use multifactor authentication.

Source: DHS CISA, USDOT, FBI, “ TraderTraitor: North Korean State-Sponsored APT Target Blockchain Companies”, Joint Cybersecurity Advisory Alert, April 20, 2022

Other Coordination Challenges?

DOI:10.1145/3372115

Software weaknesses in cryptocurrencies create unique challenges in responsible revelations.

BY RAINER BÖHME, LISA ECKEY, TYLER MOORE, NEHA NARULA, TIM RUFFING, AND AVIV ZOHAR

Responsible Vulnerability Disclosure in Cryptocurrencies

DESPITE THE FOCUS on operating in adversarial environments, cryptocurrencies have suffered a litany of security and privacy problems. Sometimes, these issues are resolved without much fanfare following a disclosure by the individual who found the hole. In other cases, they result in costly losses due to theft, exploits, unauthorized coin creation, and destruction. These experiences provide regular fodder for outrageous news headlines. In this article, we focus on the disclosure process itself, which presents unique challenges compared to other software projects.[15] To illustrate, we examine some recent disclosures and discuss difficulties that have arisen.

While Bitcoin is the best known, more than 2,000 cryptocurrencies are in circulation, collectively valued at $350 billion as of August 2020.[6] Figure 1 onceptualizes the landscape as a stack. While the etails differ, at the lowest level, each cryptocurrency system is designed to achieve common security goals: transaction integrity and availability in a highly distributed system whose participants are incentivized to cooperate.[38] Users interact with the cryptocurrency system via software "wallets" that manage the cryptographic keys associated with the coins of the user. These wallets can reside on a local client machine or be managed by an online service provider. In these applications, authenticating users and maintaining confidentiality of cryptographic key material are the central security goals. Exchanges facilitate trade between cryptocurrencies and between cryptocurrencies and traditional forms of money. Wallets broadcast cryptocurrency transactions to a network of nodes, which then relay transactions to miners, who in turn validate and group them together into blocks that are appended to the blockchain.

Not all cryptocurrency applications revolve around payments. Some cryptocurrencies, most notably Ethereum, support "smart contracts" in which general-purpose code can be executed with integrity assurances and recorded on the distributed ledger. An explosion of token systems has appeared, in which particular functionality is expressed and run on top of a cryptocurrency.[12] Here, the promise is that business logic can be specified in the smart contract and confidently executed in a distributed fashion.

The emergence of a vibrant ecosystem of decentralized cryptocurrencies has prompted proposals that leverage the underlying technology to construct new central bank currency[2] and corpo-

» key insights

- Cryptocurrency software is complex and vulnerabilities can be readily, and anonymously, monetized.
- Responsible vulnerability disclosure in cryptocurrencies is hard because decentralized systems, by design, give no single party authority to push code updates.
- This review of case studies informs recommendations for preventing catastrophic cryptocurrency failures.

Böhme, Rainer, et al. "Responsible vulnerability disclosure in cryptocurrencies." *Communications of the ACM* 63.10 (2020): 62-71.

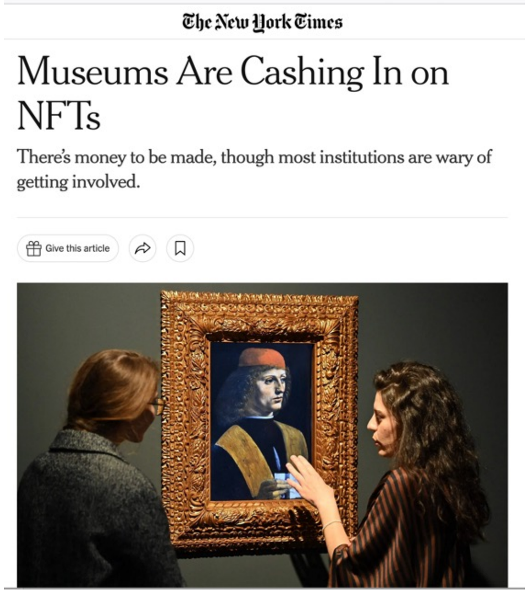
- **Decentralized Coordination of Bugs = Major Challenge**
- Insider Activity
- Market Manipulation (Wash Trading, etc.)
- Security Bugs in Smart Contracts, Client Software
- Governance (Voting) Protocol Manipulations
- Security flaws in off-chain marketplaces (such as those for buying and selling NFTs)

But if we are not launching NFTs can we just **turn it off** like P2P filesharing?

Prediction: No

Organizations pursing activities involving the underlying technology as well

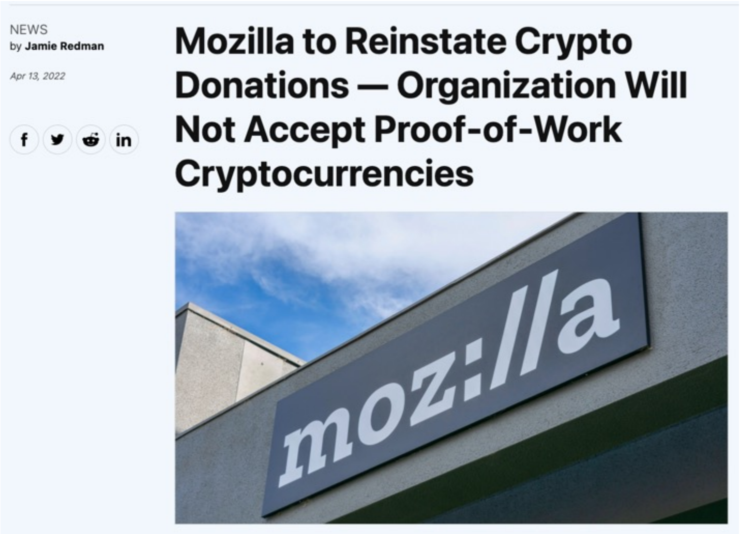
Orgs. are exploring Digital Assets fundraising, payments, and new business models



The New York Times

Museums Are Cashing In on NFTs

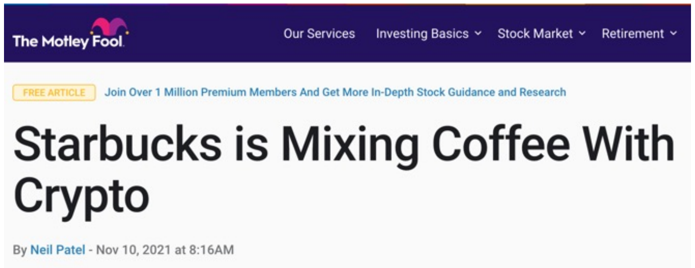
There's money to be made, though most institutions are wary of getting involved.



NEWS
by **Jamie Redman**

Apr 13, 2022

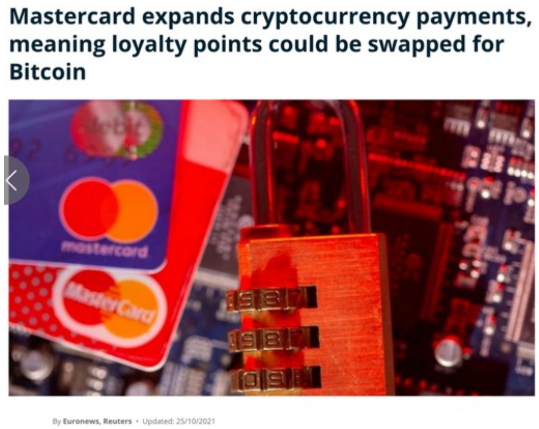
Mozilla to Reinstate Crypto Donations — Organization Will Not Accept Proof-of-Work Cryptocurrencies



FREE ARTICLE Join Over 1 Million Premium Members And Get More In-Depth Stock Guidance and Research

Starbucks is Mixing Coffee With Crypto

By Neil Patel - Nov 10, 2021 at 8:16AM



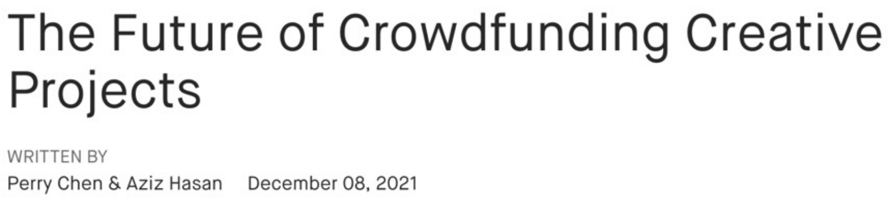
Mastercard expands cryptocurrency payments, meaning loyalty points could be swapped for Bitcoin

By **Euronews, Reuters** • Updated: 25/10/2021

Sources:

- Reyburn, Scott, "Museums Are Cashing In on NFTs", The New York Times, March 25, 2022
- Patel, Neil, "Starbucks is Mixing Coffee With Crypto", The Motley Fool, November 10, 2021
- Reuters, "Mastercard expands cryptocurrency payments, meaning loyalty points could be swapped for Bitcoin", Euronews, Reuters, October 25, 2021
- Redman, Jamie, "Mozilla to Reinstate Crypto Donations — Organization Will Not Accept Proof-of-Work Cryptocurrencies", April 13, 2022

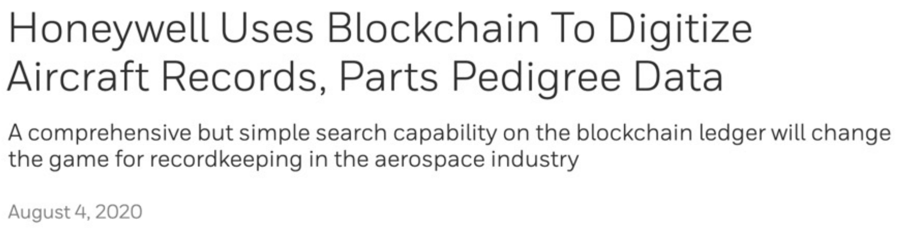
And Blockchain Projects Beyond Payments



The Future of Crowdfunding Creative Projects

WRITTEN BY

Perry Chen & Aziz Hasan December 08, 2021



Honeywell Uses Blockchain To Digitize Aircraft Records, Parts Pedigree Data

A comprehensive but simple search capability on the blockchain ledger will change the game for recordkeeping in the aerospace industry

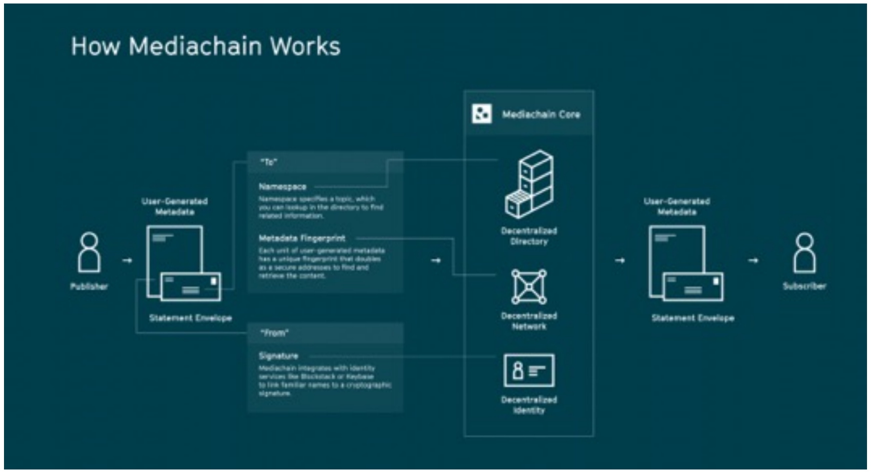
August 4, 2020

And not just for currency but other business related tasks as well

Sources:

- Chen, Peter and Hasan, Aziz, “The Future of Crowdfunding Creative Projects”, Kickstarter Blog, December 08, 2021
- “Honeywell Uses Blockchain To Digitize Aircraft Records, Parts Pedigree Data”, Honeywell Press Release, August 4, 2020

Source: https://burstiq.com/


How Mediachain Works
Publisher
User-Generated Metadata
Statement Envelope
"To"
Namespace
Namespace specifies a topic, which you can lookup in the directory to find related information.
Metadata Fingerprint
Each unit of user-generated metadata has a unique fingerprint that doubles as a secure addresses to find and retrieve the content.
"From"
Signature
Mediachain integrates with identity services like Blockstack or Keybase to link familiar names to a cryptographic signature.
Mediachain Core
Decentralized Directory
Decentralized Network
Decentralized Identity
User-Generated Metadata
Statement Envelope
Subscriber

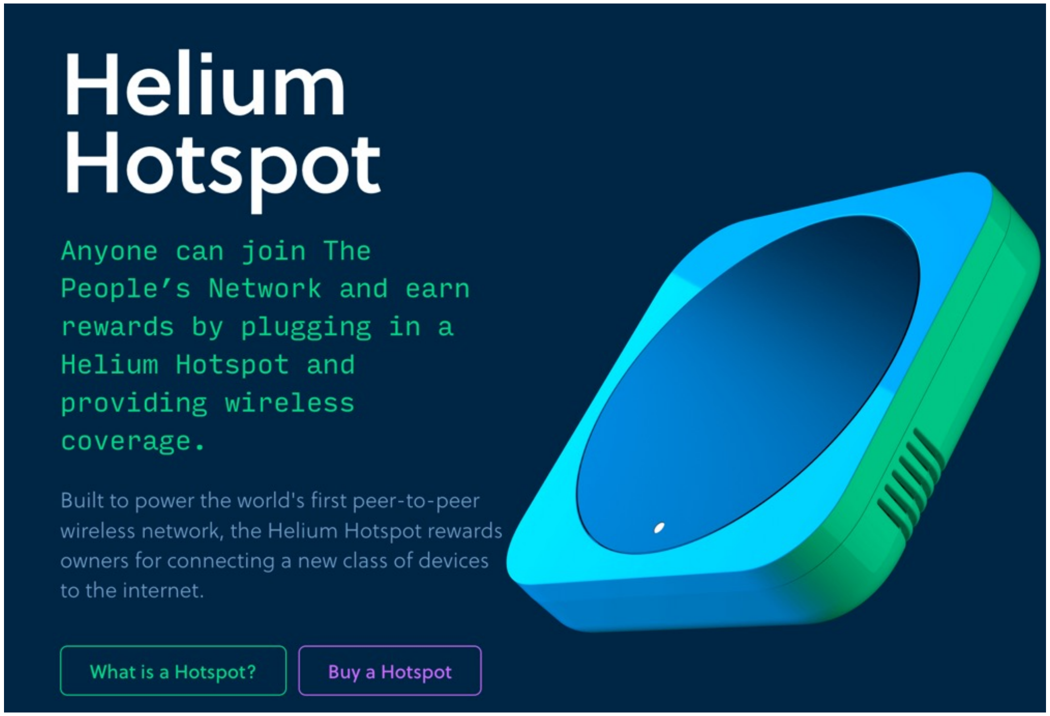
Source: http://www.mediachain.io/

Source: https://xage.com/

Source: https://propy.com/browse/

Not to mention new market entrants with blockchain based solutions

The future isn’t entirely clear



Helium Hotspot

Anyone can join The People’s Network and earn rewards by plugging in a Helium Hotspot and providing wireless coverage.

Built to power the world's first peer-to-peer wireless network, the Helium Hotspot rewards owners for connecting a new class of devices to the internet.

Image Source: https://www.helium.com/

“Helium – Venture Capital Con Job or Viable Business ?”

Sources: Ferro, Greg, ““Helium – Venture Capital Con Job or Viable Business ?”, June 20, 2019

Remediations?

Remediation: Awareness, Training, Experience, Tools, Processes

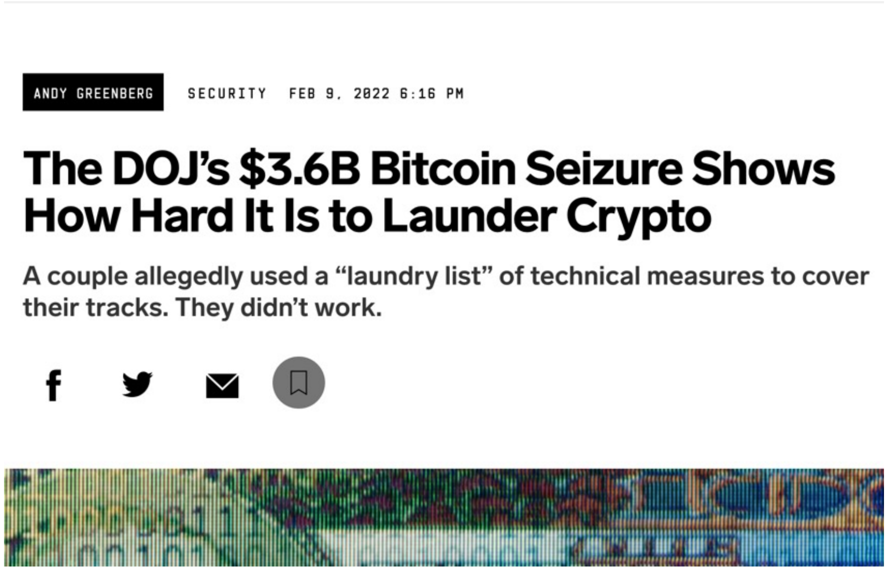
- Knowledge of how things work such as:
  - Tornado Cash
  - Lightning Network
  - Exchanges
- Skills Acquisition
  - Smart Contract Development
  - Offensive Security for Blockchain
  - Link Analysis (Pseudo anonymity)
  - Decentralized Network Technology
  - DAOs, Discord

- Blockchain Forensic Analysis
- Fund Tracking & Analysis Tools (Analytics)
  - Chainalysis, and others
- Blockchain Threat Data Sources
- Smart Contract Code Auditing & Testing Tools
- Bytecode analysis tools
- Code Templates
  - OpenZeppellin and others
- Many more …

General Blockchain Technical Skills (to have or be able to call up)

- Be able to interact with Public Blockchains
  - Could be via API, or running a node
- Be familiar with the types of data available on various public Blockchain Networks and Host Logs
- Understand different Network protocols for performing Peer Discovery and communication
  - Examples include “Eclipse” attacks (surround a node) and many more
- Be able to access, read, and interact with a public Smart Contract
- Knowledge of social and economic attacks on crypto ecosystems and users
  - Phishing scams, frauds, rug-pulls, impersonation, key theft, and more
- Blockchain Threat Intelligence and News
  - Such as https://newsletter.blockthreat.io/

Analysis can help with investigations

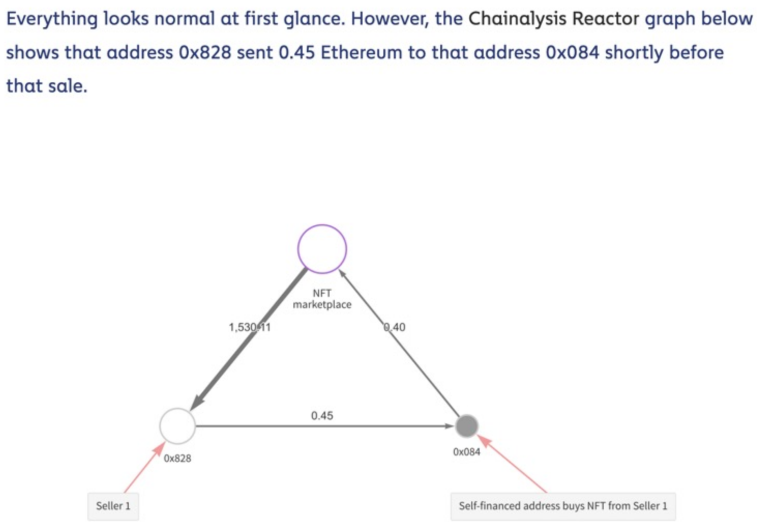


ANDY GREENBERG SECURITY FEB 9, 2022 6:16 PM

The DOJ's $3.6B Bitcoin Seizure Shows How Hard It Is to Launder Crypto

A couple allegedly used a "laundry list" of technical measures to cover their tracks. They didn't work.

Source: Greenberg, Andy, "The DOJ's $3.6B Bitcoin Seizure Shows How Hard It Is to Launder Crypto", Wired, February 9, 2022



Everything looks normal at first glance. However, the Chainalysis Reactor graph below shows that address 0x828 sent 0.45 Ethereum to that address 0x084 shortly before that sale.

Link analysis can help discover NFT Wash Trading and other market manipulation

Source: Chainalysis Team, "Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class ", February 2, 2022

More Advanced

- Be able to write, deploy, and/or analyze a Smart Contract
- Have knowledge of types of attacks on smart contracts (e.g. reentrancy), secure coding best practices and tools
- Flash Loans, Price Manipulations
- Client code analysis
- Wallet software analysis
- Crypto related Malware analysis (key theft, cryptojacking, etc.)

Speculation on future impacts

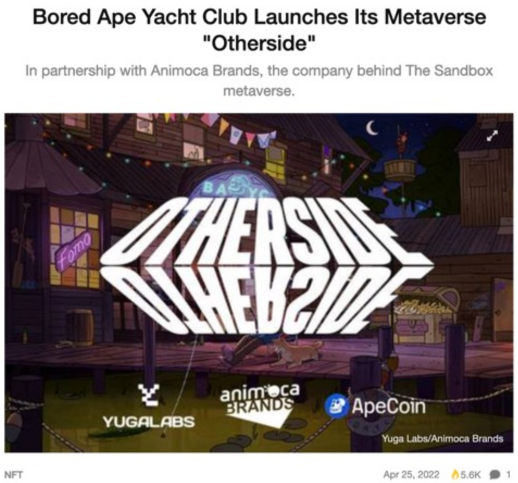
Increases in different contexts leads to a need for more specialized Defender skills

Evolution of Blockchains – DAOs for Research Centers

New combinations of internet services and Blockchains such as “The Metaverse”

What if it turns out to be more like email than P2P filesharing for Incident Responders?

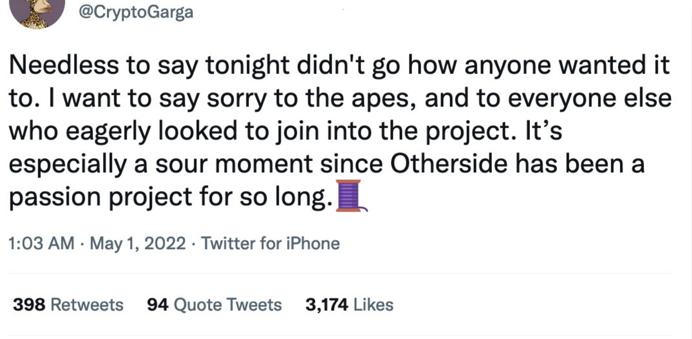
One example: Metaverse may mean new types of incidents and outages



Bored Ape Yacht Club Launches Its Metaverse "Otherside"

In partnership with Animoca Brands, the company behind The Sandbox metaverse.

← Thread



Garga.eth
@CryptoGarga

Needless to say tonight didn't go how anyone wanted it to. I want to say sorry to the apes, and to everyone else who eagerly looked to join into the project. It's especially a sour moment since Otherside has been a passion project for so long.🧵

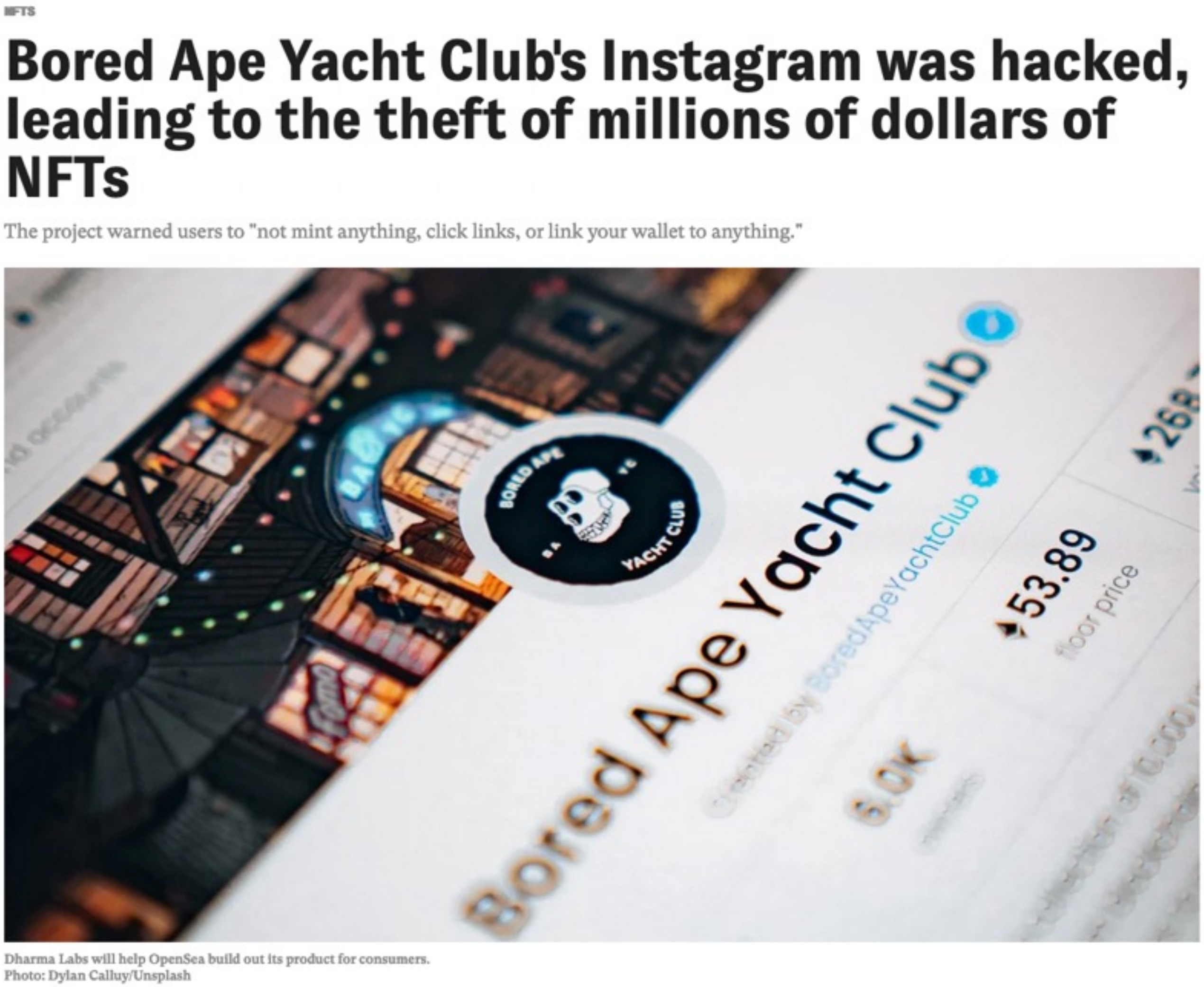
1:03 AM · May 1, 2022 · Twitter for iPhone

398 Retweets 94 Quote Tweets 3,174 Likes

- *Otherside* metaverse project
- Increased transaction volumes strain the network
- Increases transaction fees (”Gas)
- Users can lose low fee estimates outright
- Many project supporters and general Ethereum network users upset as well.
- Attempts to return funds to community members who lost out

Sources:

- Parkhouse, Arthur, 'Bored Ape Yacht Club Launches Its Metaverse "Otherside"', April 25, 2022
- Garga.eth [@CryptoGarga] (2022, May, 1). *Needless to say tonight didn't go how anyone wanted it to….*[Tweet]. Twitter. https://twitter.com/CryptoGarga/status/1520629889359089665



NFTS

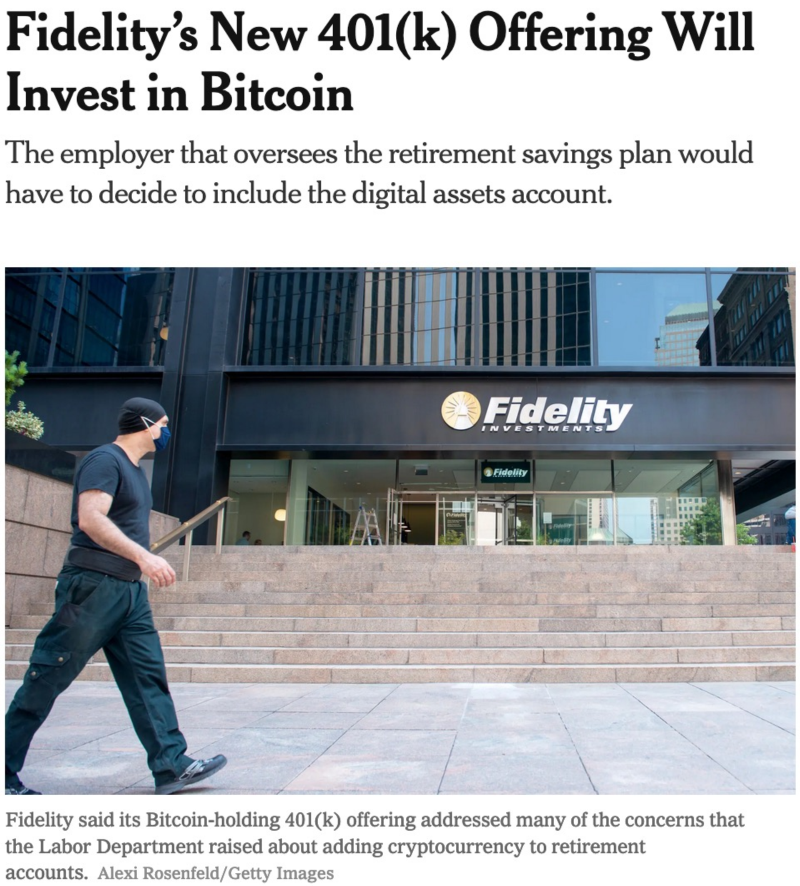
Bored Ape Yacht Club's Instagram was hacked, leading to the theft of millions of dollars of NFTs

The project warned users to "not mint anything, click links, or link your wallet to anything."

Dharma Labs will help OpenSea build out its product for consumers.
Photo: Dylan Calluy/Unsplash

Source: Rubio-Licht, Nat, “Bored Ape Yacht Club's Instagram was hacked, leading to the theft of millions of dollars of NFTs”, Protocol, April 25, 2022

Closing Remarks



Fidelity's New 401(k) Offering Will Invest in Bitcoin

The employer that oversees the retirement savings plan would have to decide to include the digital assets account.

Fidelity said its Bitcoin-holding 401(k) offering addressed many of the concerns that the Labor Department raised about adding cryptocurrency to retirement accounts. Alexi Rosenfeld/Getty Images

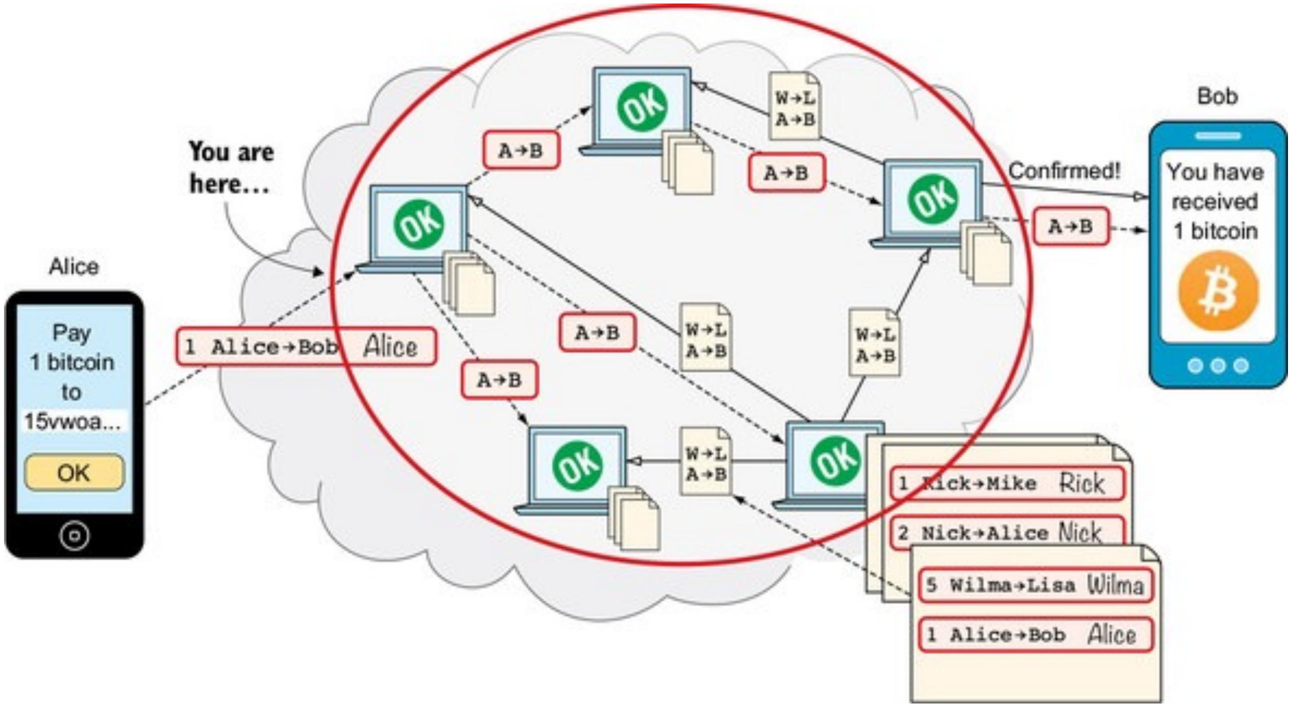
Source: Bernard, Tara Siegel, "Fidelity's New 401(k) Offering Will Invest in Bitcoin", The New York Times, April 26, 2022

- Increase activity for Crypto, Smart Contracts, and other Blockchain
- Incidents with blockchain and smart contracts require new approaches
- Threat actors are motivated and active
- Increased Coordination Challenges
- *Metaverse* brings additional incidents and types
- Can not ignore it or turn it off

End

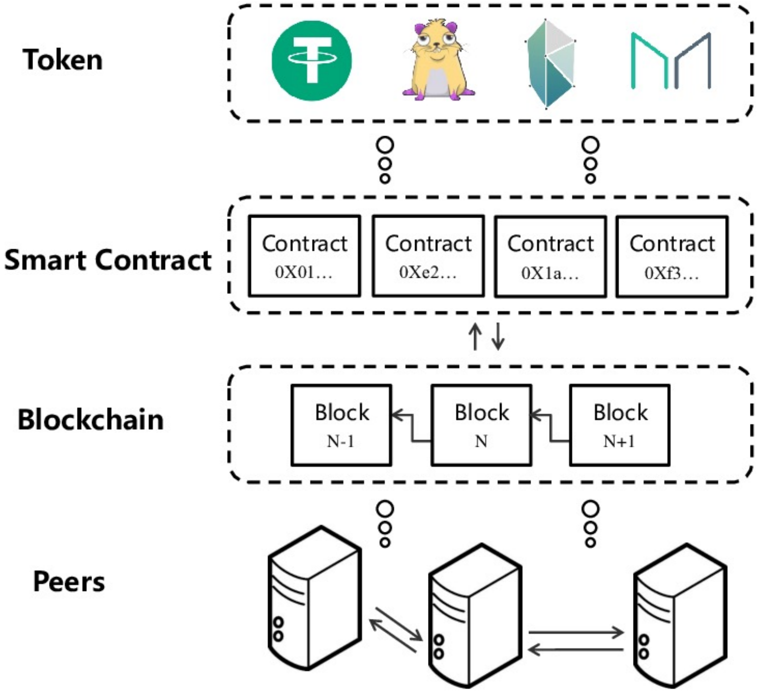
Appendix

Blockchain Network(s)

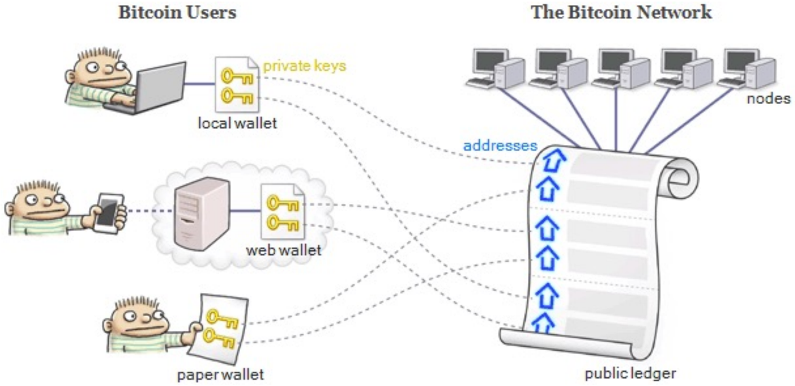


https://livebook.manning.com/book/grokking-bitcoin/chapter-8/6

Ecosystem Overview



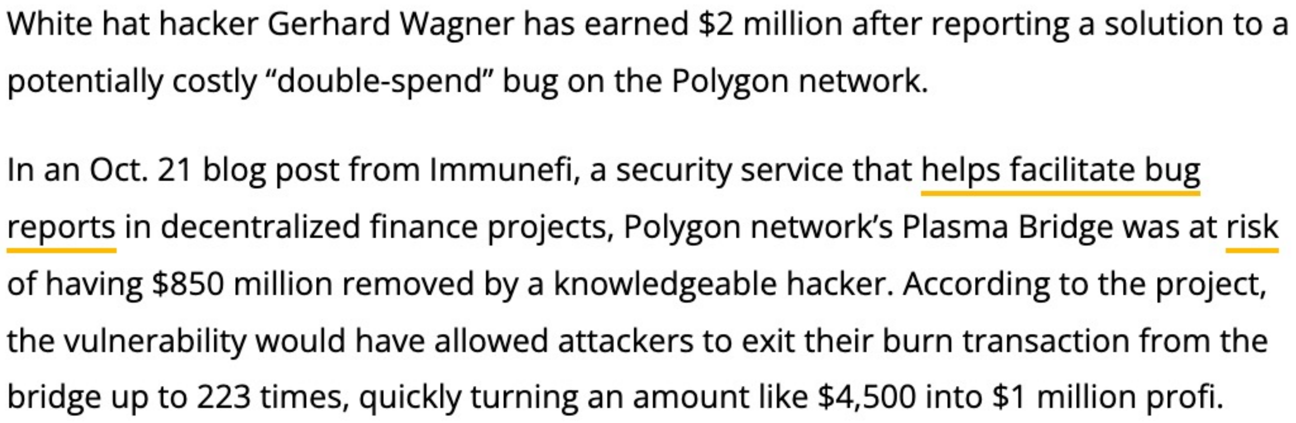
https://www.researchgate.net/figure/Overview-of-Ethereum-Blockchain_fig1_337005478



https://preshing.com/20140127/what-is-a-bitcoin-really/

Another Smart Contract Example: Polygon pays $2M bounty on bug which could have compromised $850M in user funds

Probably from "using someone else's code and not having a 100% understanding of what it does."



White hat hacker Gerhard Wagner has earned $2 million after reporting a solution to a potentially costly "double-spend" bug on the Polygon network.

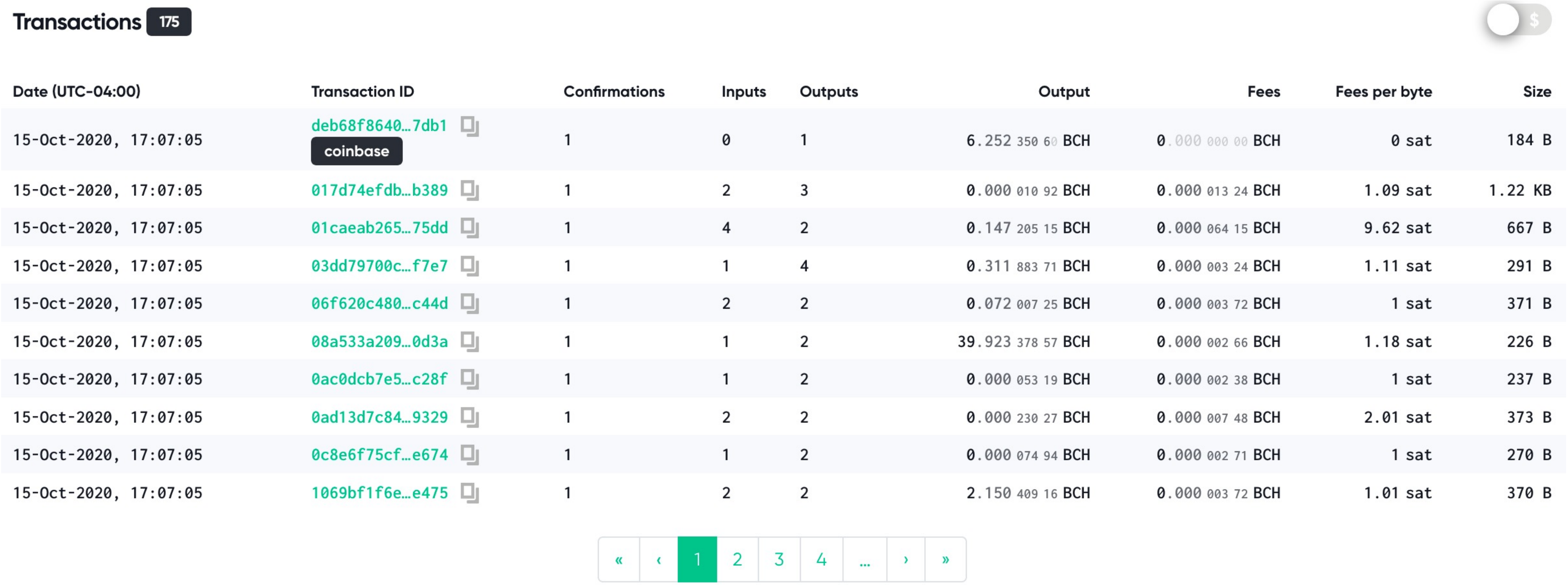
In an Oct. 21 blog post from Immunefi, a security service that helps facilitate bug reports in decentralized finance projects, Polygon network's Plasma Bridge was at risk of having $850 million removed by a knowledgeable hacker. According to the project, the vulnerability would have allowed attackers to exit their burn transaction from the bridge up to 223 times, quickly turning an amount like $4,500 into $1 million profi.

October 22, 2021

https://cointelegraph.com/news/polygon-pays-2m-bounty-on-bug-which-could-have-compromised-850m-in-user-funds

What is inside of a “Block”?

contains transactions (transfer BCH from one address to another)
Block #657287

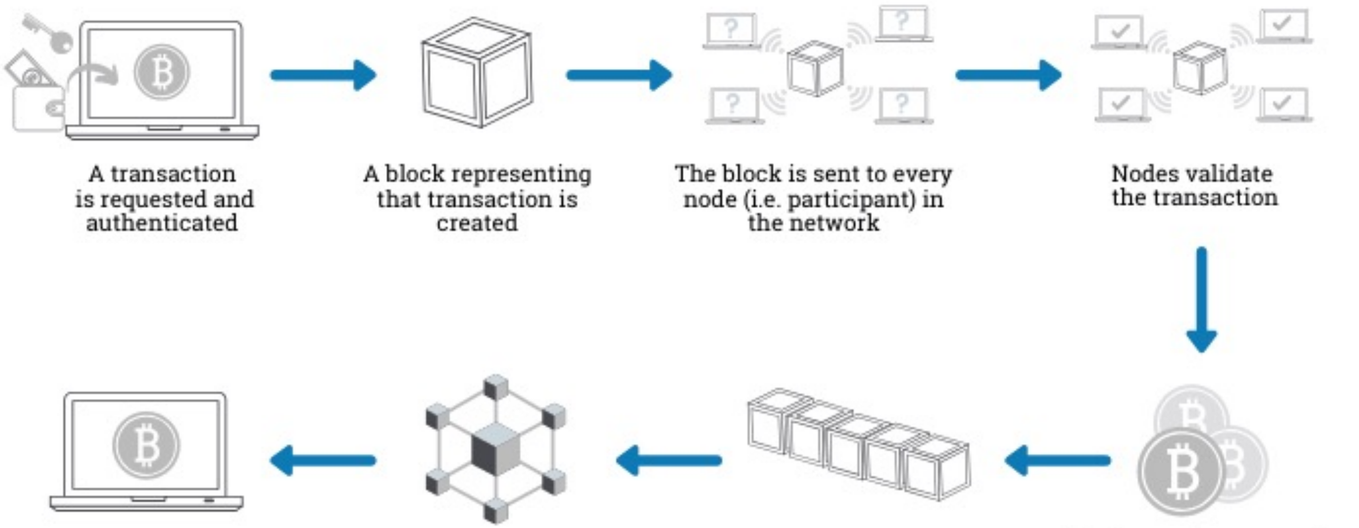


Transactions 175

Date (UTC-04:00)	Transaction ID	Confirmations	Inputs	Outputs	Output	Fees	Fees per byte	Size
15-Oct-2020, 17:07:05	deb68f8640…7db1 coinbase	1	0	1	6.252 350 60 BCH	0.000 000 00 BCH	0 sat	184 B
15-Oct-2020, 17:07:05	017d74efdb…b389	1	2	3	0.000 010 92 BCH	0.000 013 24 BCH	1.09 sat	1.22 KB
15-Oct-2020, 17:07:05	01caeab265…75dd	1	4	2	0.147 205 15 BCH	0.000 064 15 BCH	9.62 sat	667 B
15-Oct-2020, 17:07:05	03dd79700c…f7e7	1	1	4	0.311 883 71 BCH	0.000 003 24 BCH	1.11 sat	291 B
15-Oct-2020, 17:07:05	06f620c480…c44d	1	2	2	0.072 007 25 BCH	0.000 003 72 BCH	1 sat	371 B
15-Oct-2020, 17:07:05	08a533a209…0d3a	1	1	2	39.923 378 57 BCH	0.000 002 66 BCH	1.18 sat	226 B
15-Oct-2020, 17:07:05	0ac0dcb7e5…c28f	1	1	2	0.000 053 19 BCH	0.000 002 38 BCH	1 sat	237 B
15-Oct-2020, 17:07:05	0ad13d7c84…9329	1	2	2	0.000 230 27 BCH	0.000 007 48 BCH	2.01 sat	373 B
15-Oct-2020, 17:07:05	0c8e6f75cf…e674	1	1	2	0.000 074 94 BCH	0.000 002 71 BCH	1 sat	270 B
15-Oct-2020, 17:07:05	1069bf1f6e…e475	1	2	2	2.150 409 16 BCH	0.000 003 72 BCH	1.01 sat	370 B

https://explorer.bitcoin.com/bch/block/000000000000000000d0102fbaed12406289b4d858763abff4203a2e2085cc8b

How does a transaction get into the blockchain?



A transaction is requested and authenticated

A block representing that transaction is created

The block is sent to every node (i.e. participant) in the network

Nodes validate the transaction

Nodes receive a reward for Proof of Work, typically in cryptocurrency

The block is added to the existing blockchain

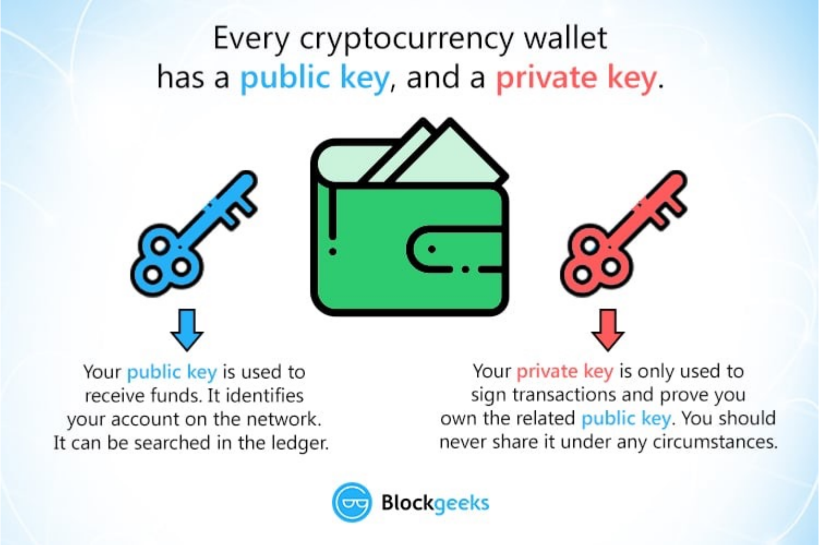
The update is distributed across the network

The transaction is complete

https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain © Euromoney Learning 2020

Blockchain – A public distributed ledger of transaction history. It is copied onto many different network nodes.

“Wallets”

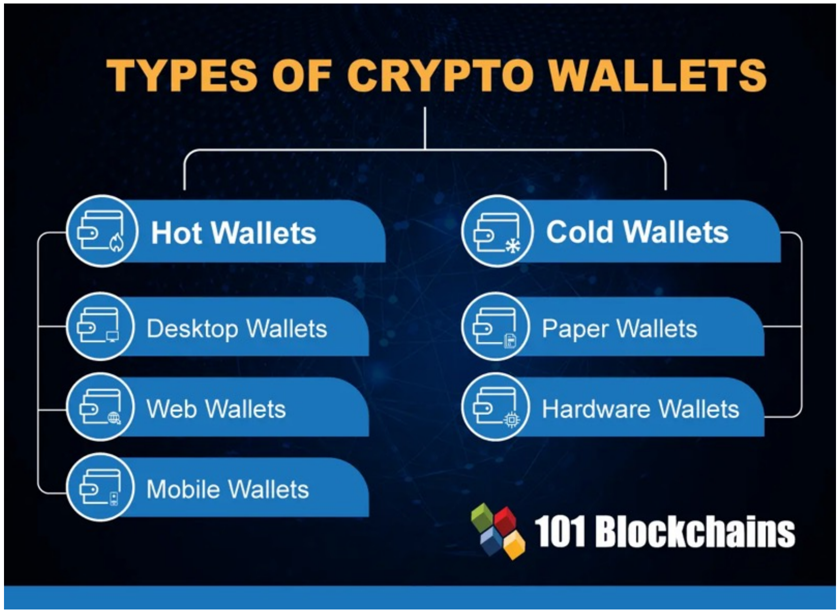


Every cryptocurrency wallet has a public key, and a private key.

Your public key is used to receive funds. It identifies your account on the network. It can be searched in the ledger.

Your private key is only used to sign transactions and prove you own the related public key. You should never share it under any circumstances.

https://blockgeeks.com/guides/cryptocurrency-wallet-guide/



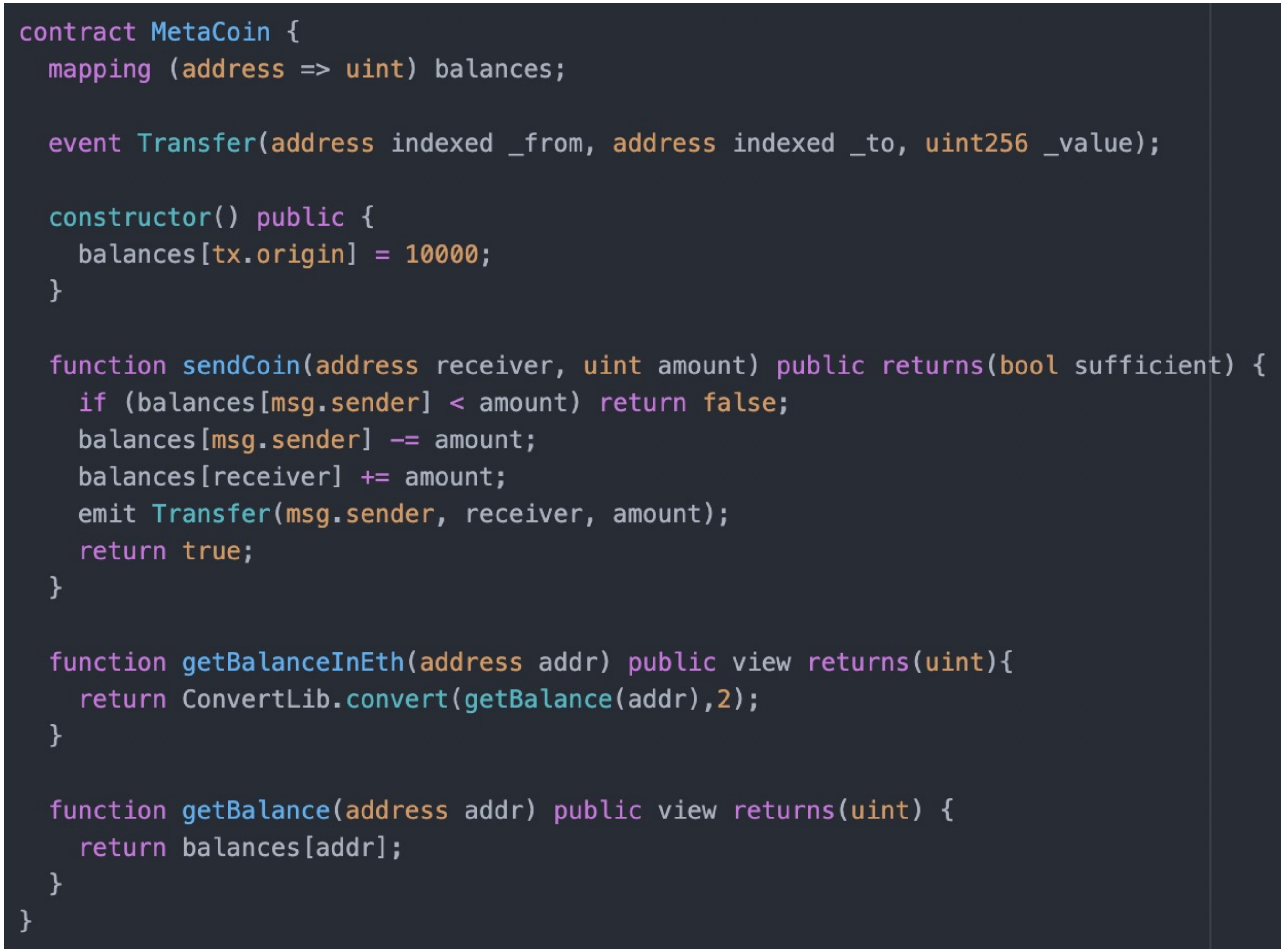
TYPES OF CRYPTO WALLETS

- Hot Wallets
  - Desktop Wallets
  - Web Wallets
  - Mobile Wallets
- Cold Wallets
  - Paper Wallets
  - Hardware Wallets

https://101blockchains.com/types-of-crypto-wallets/

Wallets – Hold user addresses, hold keys to send / receive coins / tokens, fetch/calculate balances. Some have multiple parties.

Smart Contract Example Code



```
contract MetaCoin {
  mapping (address => uint) balances;

  event Transfer(address indexed _from, address indexed _to, uint256 _value);

  constructor() public {
    balances[tx.origin] = 10000;
  }

  function sendCoin(address receiver, uint amount) public returns(bool sufficient) {
    if (balances[msg.sender] < amount) return false;
    balances[msg.sender] -= amount;
    balances[receiver] += amount;
    emit Transfer(msg.sender, receiver, amount);
    return true;
  }

  function getBalanceInEth(address addr) public view returns(uint){
    return ConvertLib.convert(getBalance(addr),2);
  }

  function getBalance(address addr) public view returns(uint) {
    return balances[addr];
  }
}
```

https://trufflesuite.com/boxes/metacoin/index.html

Build your own coin or Token

- sendCoin (sender, receiver, amt)
- getBalance(addr)
- **The Ethereum Blockchain will record all issuances, all sends, and all receives**

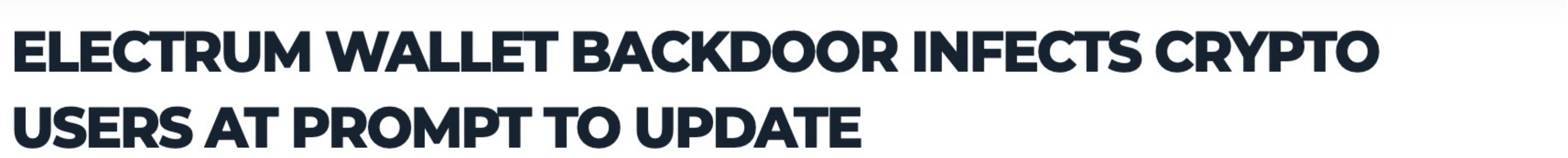
Examples of Blockchain Organizations

- **Exchanges** – Organizations that exchange Crypto for other currency (either other crypto or “fiat”)
- **DAOs & Governance** – Distributed Autonomous Organizations. Use blockchain technology to raise funds, facilitate decisions via voting.
- **Decentralized Exchanges (DEX)** – Exchanges without a centralized organizational presence, often via Smart Contract
- **Miners** – Nodes/Organizations that validate transactions to earn cryptocurrency rewards

Other Terms

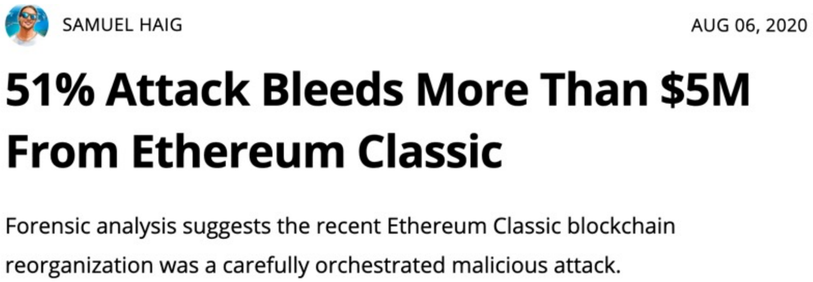
- Tornado Cash – a mixer for hiding stolen coins
- Lightning Network – A sub-network that sits on top of the Bitcoin network to make payments faster (Layer 2) but still have some amount of verification/validation assurances.
- Exchanges – Places to sell Crypto for Fiat, cash (or other crypto)
- Chainalysis, and others – Organizations and tools for performing analysis

Other Incident Examples:
Humans are usually easier to attack than hash power



ELECTRUM WALLET BACKDOOR INFECTS CRYPTO USERS AT PROMPT TO UPDATE

An unexpected prompt to updates the software for security reasons triggers a backdoor opening. Rather than pinging official Electrum servers, it’s rerouted to the hacker’s servers, which allows access to the user’s wallet.



SAMUEL HAIG AUG 06, 2020

51% Attack Bleeds More Than $5M From Ethereum Classic

Forensic analysis suggests the recent Ethereum Classic blockchain reorganization was a carefully orchestrated malicious attack.

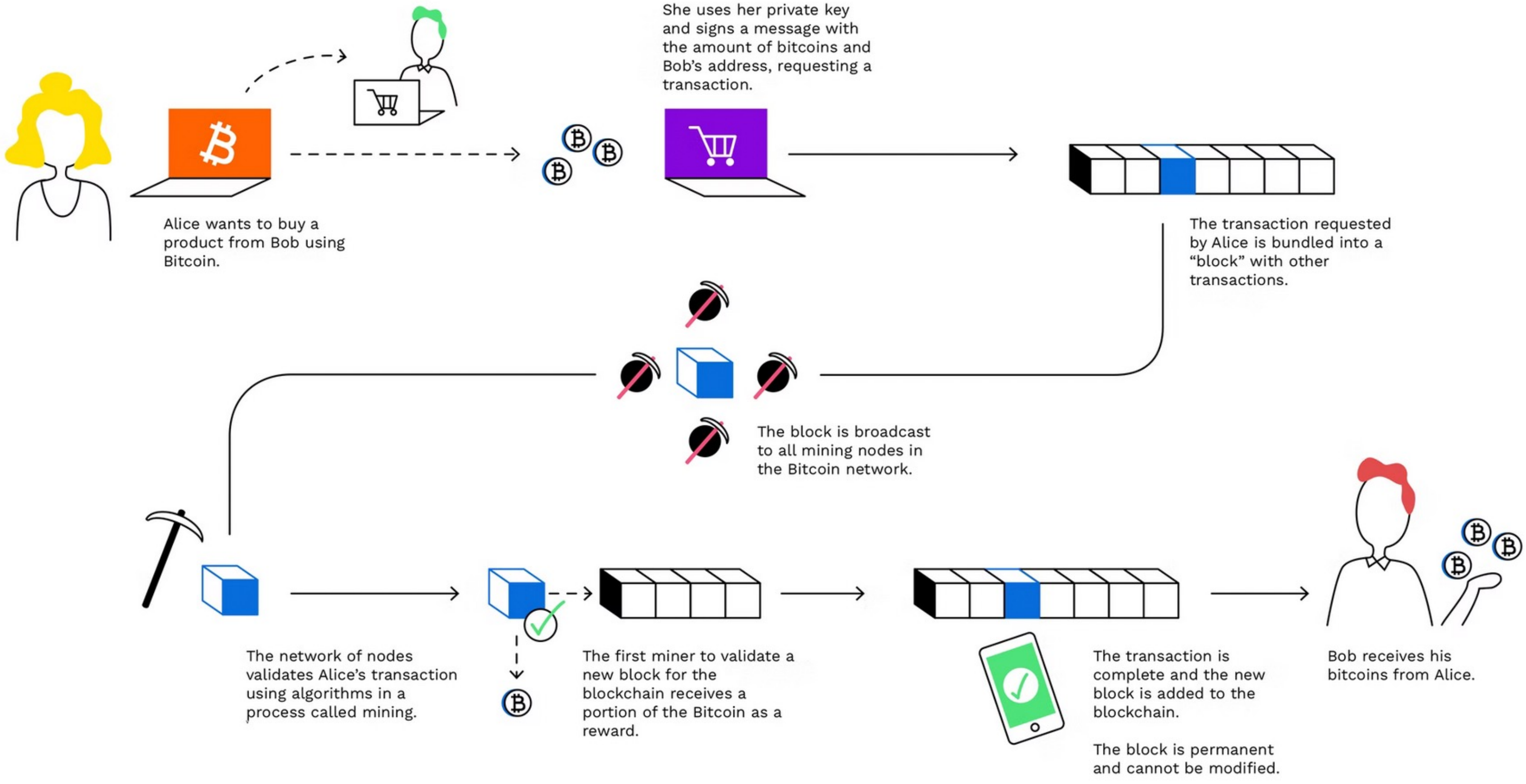
Sources:
https://bitcoinist.com/this-ongoing-bitcoin-wallet-hack-has-stolen-22-million-in-btc/
https://cointelegraph.com/news/51-attack-bleeds-more-than-5m-from-ethereum-classic

Questions

1. Introduction - What might be the impact of crypto on IR?
2. InfoSec news from the crypto world – present examples of IR and crypto related problems
3. Make parallels to impacts of other decentralized technologies on IR.
4. Challenges - Talk about challenges of applying IR to crypto today
5. Future Questions - Pose questions about the future

What is Bitcoin Mining?

How Bitcoin Transactions work



Alice wants to buy a product from Bob using Bitcoin.

She uses her private key and signs a message with the amount of bitcoins and Bob's address, requesting a transaction.

The transaction requested by Alice is bundled into a "block" with other transactions.

The block is broadcast to all mining nodes in the Bitcoin network.

The network of nodes validates Alice's transaction using algorithms in a process called mining.

The first miner to validate a new block for the blockchain receives a portion of the Bitcoin as a reward.

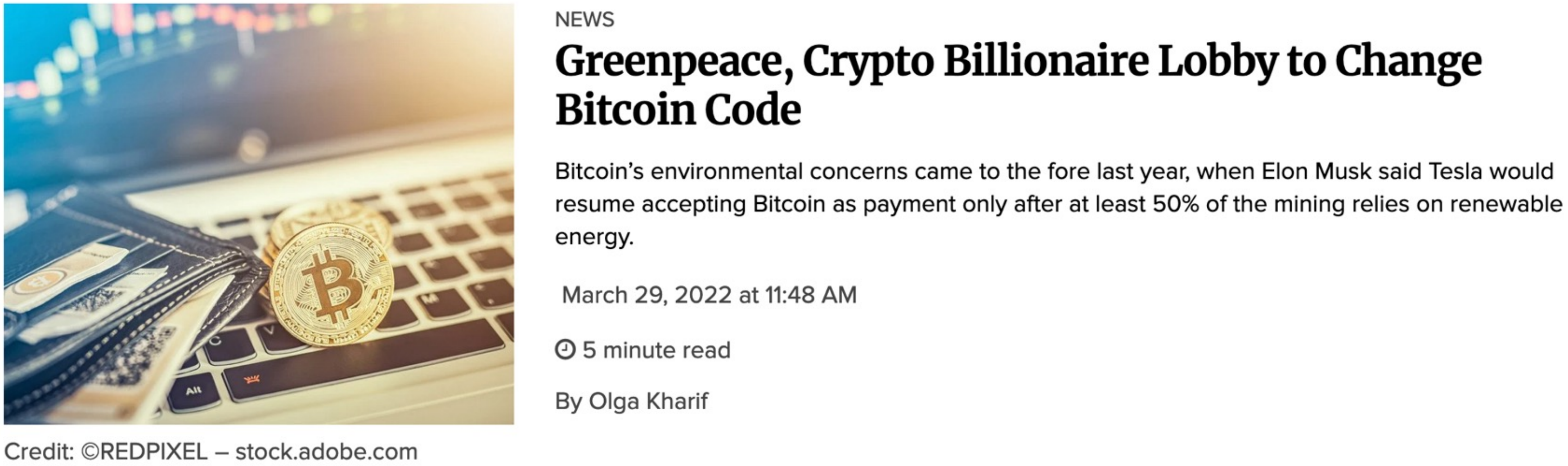
The transaction is complete and the new block is added to the blockchain.

The block is permanent and cannot be modified.

Bob receives his bitcoins from Alice.

Source: https://www.bitpanda.com/academy/en/lessons/what-is-bitcoin-mining-and-how-does-mining-work/

Is it “decentralized”?



NEWS

Greenpeace, Crypto Billionaire Lobby to Change Bitcoin Code

Bitcoin’s environmental concerns came to the fore last year, when Elon Musk said Tesla would resume accepting Bitcoin as payment only after at least 50% of the mining relies on renewable energy.

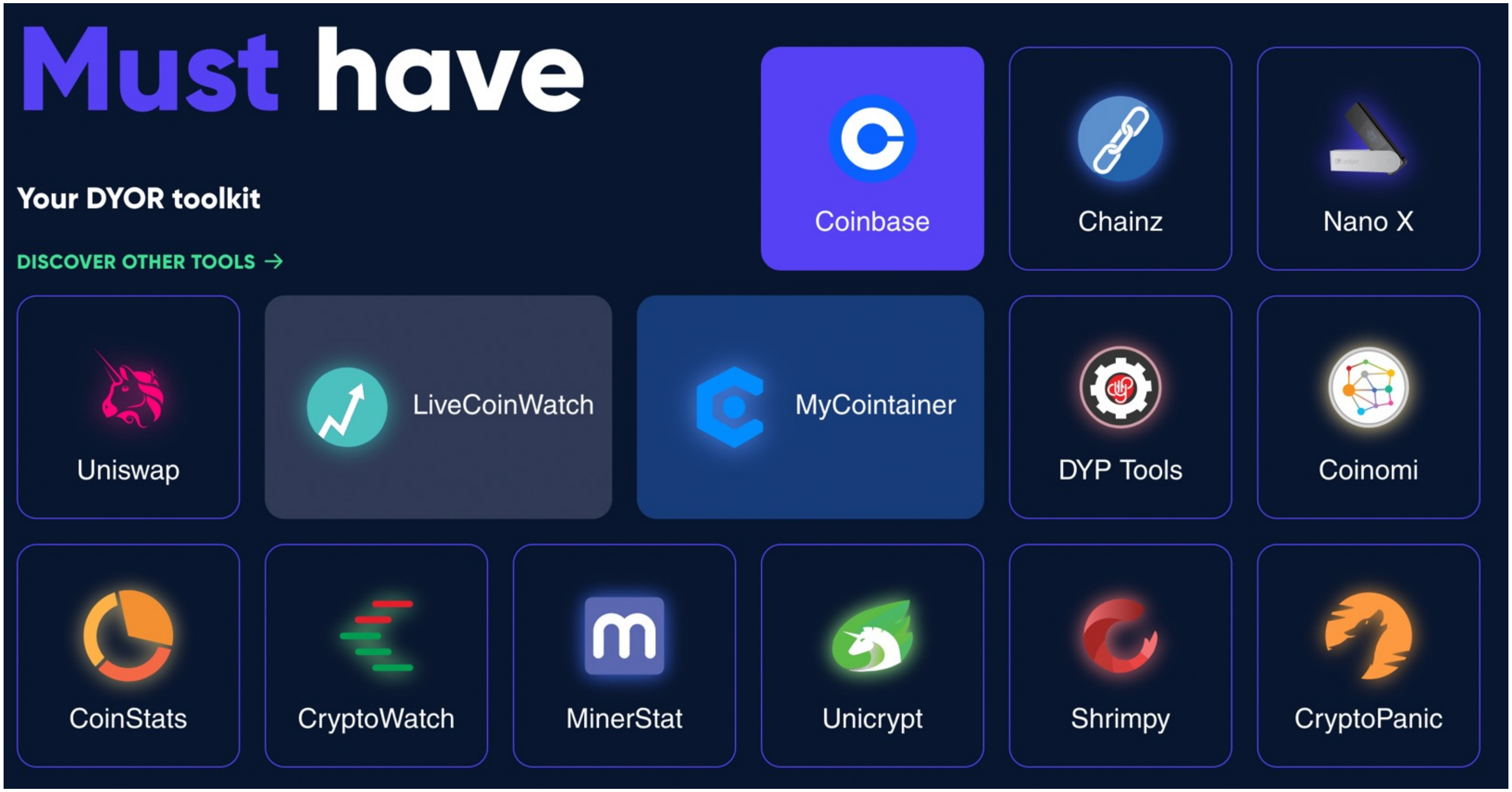
March 29, 2022 at 11:48 AM

5 minute read

By Olga Kharif

Credit: ©REDPIXEL – stock.adobe.com

- **“The campaign believes that about 50 key miners, crypto exchanges and core developers have the power to change Bitcoin’s code.”**



Must have

Your DYOR toolkit

DISCOVER OTHER TOOLS →

Coinbase

Chainz

Nano X

Uniswap

LiveCoinWatch

MyCointainer

DYP Tools

Coinomi

CoinStats

CryptoWatch

MinerStat

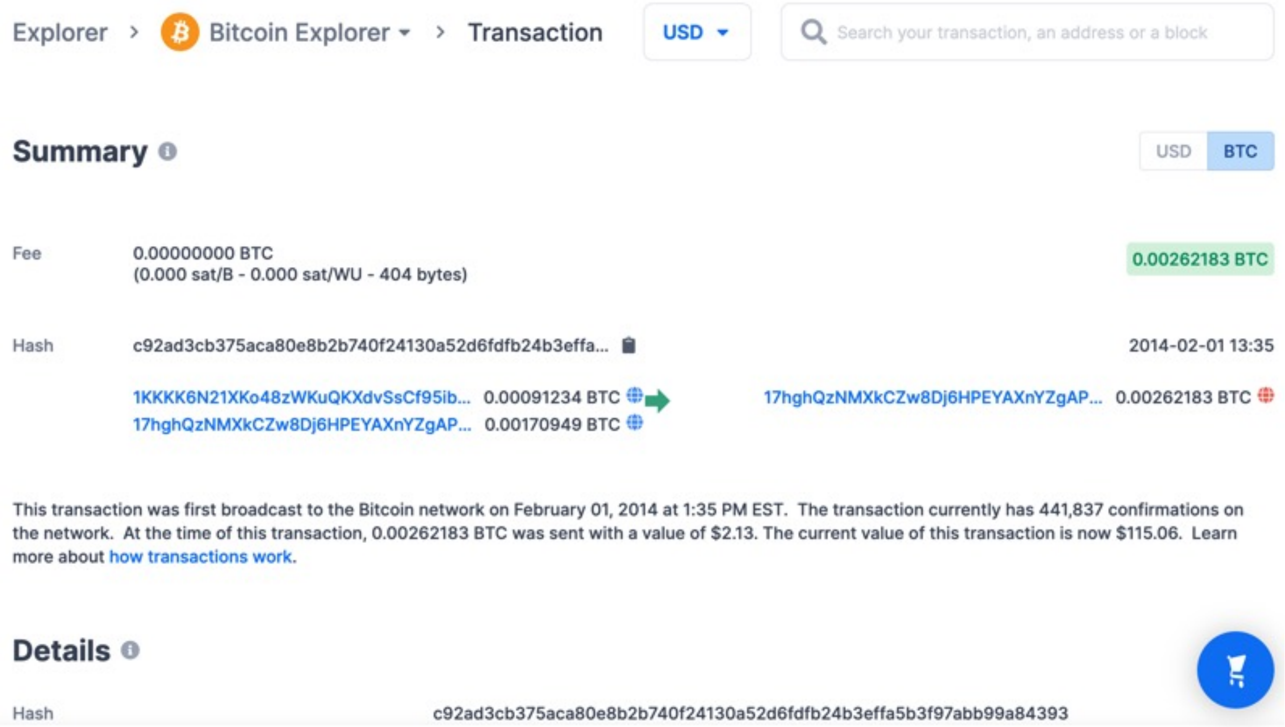
Unicrypt

Shrimpy

CryptoPanic

Will you need to use all of these? Or even know what they all are?

The Address is used to write entries into the Ledger (Send / Receive)



Explorer › Bitcoin Explorer › Transaction
USD
Search your transaction, an address or a block

Summary

Fee 0.00000000 BTC
(0.000 sat/B - 0.000 sat/WU - 404 bytes)

0.00262183 BTC

Hash c92ad3cb375aca80e8b2b740f24130a52d6fdfb24b3effa...

2014-02-01 13:35

1KKKK6N21XKo48zWKuQKXdvSsCf95ib... 0.00091234 BTC
17hghQzNMXkCZw8Dj6HPEYAXnYZgAP... 0.00170949 BTC
→ 17hghQzNMXkCZw8Dj6HPEYAXnYZgAP... 0.00262183 BTC

This transaction was first broadcast to the Bitcoin network on February 01, 2014 at 1:35 PM EST. The transaction currently has 441,837 confirmations on the network. At the time of this transaction, 0.00262183 BTC was sent with a value of $2.13. The current value of this transaction is now $115.06. Learn more about how transactions work.

Details

Hash c92ad3cb375aca80e8b2b740f24130a52d6fdfb24b3effa5b3f97abb99a84393

Here is the transaction of someone using the key to steal the bitcoins. (Now worth over $100)…
https://www.blockchain.com/btc/tx/c92ad3cb375aca80e8b2b740f24130a52d6fdfb24b3effa5b3f97abb99a84393